

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-18852

(43) 公開日 平成9年(1997)1月17日

(51) Int.Cl.⁶

H 0 4 N 7/16
7/167

識別記号

庁内整理番号

F I

H 0 4 N 7/16
7/167

技術表示箇所

C

審査請求 未請求 請求項の数7 O L (全9頁)

(21) 出願番号 特願平7-166231

(22) 出願日 平成7年(1995)6月30日

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 鈴木 敏彰

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

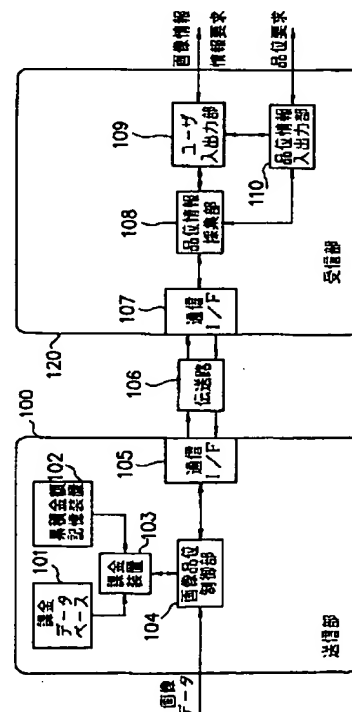
(74) 代理人 弁理士 國分 孝悦

(54) 【発明の名称】 通信装置及び通信システム

(57) 【要約】

【目的】 利用者に提供される画像情報の品位に応じた金額を利用者に課金する。

【構成】 利用者は受信部120のユーザ入出力部109により情報を要求すると共に、品位情報入出力部110により画像の品位を選択する。これらの情報は送信部100に送られ、画像品位制御部104は入力画像データを選択された品位に応じて明度、彩度、色相の階調を制御して受信部120に送信する。これと共に、課金装置103は課金データベース101から送信した画像の品位に応じた金額を取得し、これを累積金額記憶装置102にそれまでの金額に累積して記憶させ、利用者に対する課金額とする。



【特許請求の範囲】

【請求項1】 画像を含む情報を送信する送信手段と、上記画像の品位に応じた金額を上記情報の受信者に課金する課金手段とを備えた通信装置。

【請求項2】 上記情報を受信する受信手段を設けると共に、この受信手段に、上記画像の品位を選択する選択手段を設けた請求項1記載の通信装置。

【請求項3】 上記送信手段に、上記情報を暗号化する暗号化手段を設けると共に、上記受信手段に、上記暗号化された情報を復号する復号手段を設けた請求項2記載 10の通信装置。

【請求項4】 上記受信手段に、上記選択手段による選択情報を暗号化する暗号化手段を設けると共に、上記送信手段に、上記暗号化された選択情報を復号する復号手段を設けた請求項2記載の通信装置。

【請求項5】 上記暗号化手段における処理時間を測定する測定手段を設け、上記課金手段は上記測定手段で測定した時間に応じた課金を行うようにした請求項3又は4記載の通信装置。

【請求項6】 上記復号手段における処理時間を測定する測定手段を設け、上記課金手段は上記測定手段で測定した時間に応じた課金を行うようにした請求項3又は4記載の通信装置。 20

【請求項7】 ネットワークを介して画像情報を通信する通信システムであって、

上記画像情報の受信側は、受信すべき画像情報の画像品位を指定する指定手段を有し、

送信者は、受信側にて指定された画像品位に応じた画像情報を送信するとともに、この画像品位に応じて課金を行う課金手段を有することを特徴とする通信システム。 30

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、動画画像データ、静止画像データ、音声データ、コンピュータデータ等の情報を伝送するマルチメディアネットワーク等で用いられる通信装置及び通信システムに関し、特に情報の提供に対する課金に関するものである。

【0002】

【従来の技術】 近年、幹線通信網における光ファイバネットワークの整備、ケーブルテレビシステムの普及、衛星通信の実用化、ローカルエリアネットワークの普及等に伴い、このような通信網を利用して種々な情報を提供し、その情報の内容及び量に応じて料金を徴収する、いわゆる情報サービス産業が増大している。このようなサービスにおいては、提供した情報に対する課金を適切に行うことが重要となる。しかしながら、従来の課金方式はケーブルテレビシステムや衛星放送のように、使用頻度に無関係な月極の課金方式であったり、または、コンピュータの利用サービスのように、情報の種類や質に無関係な使用頻度（または使用時間）のみを計数した課金 50

方式であることが多かった。

【0003】 また近年、次世代通信方式であるATM (Asynchronous Transfer Mode: 非同期転送モード) の研究開発が活発化してきている。ATMは、情報をセルとよばれる固定長のバケットに分割して伝送する方式であり、音声や映像あるいはコンピュータデータを、同一伝送路上に多重化して伝送できるため、マルチメディアネットワークを実現する重要な技術として注目されている。ATMは、B-ISDN (Broadband aspects of Integrated Services Digital Network: 広帯域ISDN) の転送方式として採用されているため、B-ISDN網の交換機に必要なATMスイッチやセル分離多重LSIなどが、通信器メーカーを中心に研究発表あるいは発売が盛んになってきている。

【0004】

【発明が解決しようとする課題】 前述のような情報やサービスの種類や質に依存しない従来の課金方式では、今後さらに広がっていくことが予想される多様な情報やサービスに対応していくことは困難である。特に、画像情報には様々な画像品位が混在し、均一の課金を行った方式では適切な課金ができず、画像の品位に応じて課金体系を変化させる技術が必須となる。即ち、受信装置が再生できる品位が個々の受信装置により異なることが考えられ、受信装置の再生能力以上の情報を与えても利用者に届かない場合がある。また、利用者が過度の情報を望まない場合が考えられる。これらの場合、伝達される画像の品位に応じた課金が必要とされる。尚、ここで画像の品位とは、単位時間当たりのフレーム数、画像の画素数、画像に含まれるそれぞれの画素の色度、画素の彩度、画素の明度といった尺度のダイナミックレンジの分解能の数を言うものとする。

【0005】 本発明は上述のような実情に鑑みてなされたものであり、利用者に提供される画像の品位に応じた課金を行うことのできる通信装置及び通信システムを得ることを目的とする。

【0006】

【課題を解決するための手段】 請求項1の発明においては、画像を含む情報を送信する送信手段と、上記画像の品位に応じた金額を上記情報の受信者に課金する課金手段とを設けている。

【0007】 請求項7の発明においては、ネットワークを介して画像情報を通信する通信システムであって、上記画像情報の受信側は、受信すべき画像情報の画像品位を指定する指定手段を有し、送信者は、受信側にて指定された画像品位に応じた画像情報を送信するとともに、この画像品位に応じて課金を行う課金手段を有する。

【0008】

【作用】 本発明によれば、利用者に提供される画像の品

位に応じた金額が利用者に課金される。また、利用者が受信する画像の品位を自ら選択することができる。

【0009】また、送信される画像やその品位を選択する情報を暗号化し、受信側で復号することにより、利用者が他の利用者になりすましたり、あるいは情報が改ざんされることを防止することができ、課金に関する情報のセキュリティを保護することができる。さらに、暗号化や復号化の処理時間を測定することにより、受信した時間に応じた課金を行うことができる。

【0010】

【実施例】図1は本発明の第1の実施例を示すブロック図である。図1において、100は画像情報を送信する送信部、120は画像情報を受信する受信部で利用者が用いる。106は送信部100と受信部120との通信に用いる伝送路である。送信部100において、101は課金データベース、102は累積金額記憶装置、103は課金装置、104は画像品位制御部、105は通信インタフェースである。受信部120において、107はインタフェース、108は品位情報採集部、109はユーザ入出力部、110は品位情報入出力部である。

【0011】図2は課金データベース101の構成を示す図である。この課金データベースは利用者に提供するための情報と、その情報の単位当たりの料金とが対応して格納されている。この情報毎に異なる単位量当たりの料金を単位料金ということにする。また、利用者が選択できるようにするため、それぞれの情報には名前が与えられているものとする。このような課金データベース101は既存のデータベースで容易に構成できる。ここでは、画像の画素の数やそれらの画素の色度の階調、彩度の階調、明度の階調、単位時間当たりのフレーム数等を情報の量として換算し、単位料金を課金データベース101に登録している。この課金データベース101は半導体記憶装置、磁気記録装置、光記憶装置等により構成できる。

【0012】図3は累積金額記憶装置102の構成を示す図である。これは半導体記憶装置、磁気記録装置、光記憶装置等により構成できる。この累積金額記憶装置102には、利用者毎のある期間の利用料金の累積金額が記憶される。尚、一回受信する毎に課金請求する場合はこの累積金額記憶装置102は省略できる。

【0013】図4は課金装置103の構成を示す図である。これはCPU、乗算器、加算器等で構成できる。

【0014】次に動作について説明する。例えば図3の利用者Aが受信部120のユーザ入出力部109により情報要求し、同時に品位情報入出力部110により特定の画像の品位を選択し設定する。即ち、単位時間当たりのフレーム数、画素数、画像の色度の階調、彩度の階調、明度の階調等を利用者Aが設定する。これらの情報要求と品位情報とは通信インタフェース107、伝送路106を通じ、送信部100の通信インタフェース10

5を経て画像品位制御部104へ達する。画像品位制御部104では符号化されている入力画像データを、品位情報に応じて画素を間引く、あるいは色度、彩度、明度の階調を減少させるあるいは補間する等の演算を、DSPやセレクトスイッチなどを用いてデジタル信号処理で行う。また、上記品位情報は課金装置103へ入力される。

【0015】課金装置103は課金データベース104と累積金額記憶装置102から、それぞれ単位料金と累積金額とを採集して演算器により図4に示す式に基づき累積金額を算出し累積金額記憶装置102に記憶させる。一方、画像品位制御部104で、上述のように画像処理されて適切な品位に調整された画像情報は、通信インタフェース105、伝送路106を通じ、受信部120の通信インタフェース107を経て品位情報採集部107へと伝達される。ここで送られて来た画像情報について単位時間当たりのフレーム数、画素数、色度と彩度と明度を演算することにより品位を測定される。測定された品位が利用者Aの要求品位と比較された後、上記画像情報がユーザ入出力部109を介して利用者Aに届けられる。尚、受信部120で画像品位を比較しないようにしてもよく、その場合は、品位情報採集部108と品位情報入出力部110とを省略することができる。

【0016】尚、本発明で言う画像品位とは画像の単位時間当たりのフレーム数、画素数、彩度、明度、色度のダイナミックレンジと階調の数により決まるもので、それぞれの項目について、より広いダイナミックレンジとより細かい階調を持つほど画像品位が高い。

【0017】図5は本発明第2の実施例を示すブロック図であり、図1と対応する部分には同一符号を付して説明を省略する。本実施例においては、図5に示すように送信部100に共通鍵暗号処理部111、時間測定部112を設けると共に受信部120に共通鍵暗号処理部113を設けている。

【0018】次に動作について説明する。ここでは不図示の公知の鍵配送法、例えばIDに基づく鍵配送法(辻井重男、笠原正雄:”暗号とセキュリティ”、昭晃堂(1990)、またはRSA暗号などの公開鍵暗号方式(池野信一、小山健二:”現代暗号論”、電子情報通信学会(1986))、または鍵管理用のデータベースなどによって共通鍵暗号処理部111、113で用いられる共通鍵は予め配送されているものとする。尚、暗号化については後述により説明する。

【0019】第1の実施例と同様に、利用者から画像送信の情報要求と品位要求とがそれぞれ受信部120のユーザ入出力部109と品位情報入出力部110とから発せられ、品位情報採集部108で要求する品位を記憶された後、共通鍵暗号処理部113で暗号化される。この暗号化情報は通信インタフェース107、伝送路106を通じ、送信部100の通信インタフェース105を

て共通鍵暗号処理部111で復号される。復号された要求情報と品位情報とは画像品位制御部104へ送られる。これと共に第1の実施例と同様に課金装置103による課金が行われる。

【0020】そして、入力画像データは画像品位制御部104で第1の実施例と同様に加工された後、共通鍵暗号処理部111で暗号化される。この暗号化された画像情報は通信インタフェース105、伝送路106、通信インタフェース107を経て共通鍵暗号処理部113で復号される。復号された画像情報は第1の実施例と同様にして利用者へ届く。

【0021】また、時間測定部112で共通鍵暗号処理部111の動作時間を測定し、画像品位制御部104を経て課金装置103へ送ることにより暗号化情報に対する課金が行われる。この場合、図2の課金データベース102には暗号化情報に対する時間当たりの単位料金が設定されており、さらに課金装置103の品位情報数には時間測定部112で測定した暗号処理時間を設定する。また、復号処理時間を測定し、その時間に応じて課金することもできる。

【0022】図6は本発明の第3の実施例を示す。図6において、601はATMにより画像データ等の各種符号化データを転送するATMネットワーク、602と603はイーサネット(EtherNet)等によりATM以外のモードでデータを転送するローカルエリアネットワーク(LAN)、604はATMネットワーク601に接続され、画像データを扱うファクシミリ装置、605は内部にページメモリを有し、受信した画像データに基づいた像形成を行うカラープリンタである。606はカラーキャナ、カラープリンタを含むカラー複写機で、カラーキャナで読み取った原稿の画像データが書き込まれるページメモリ、ページメモリに書き込まれたデータを読み出してプリンタに供給する回路を含む。

【0023】607はATMネットワーク601を介して入力される画像データを一旦蓄えるファイルサーバ、608はファイルサーバ607にデータを入出力するためのワークステーション、609はATMネットワーク601と接続されるパソコンであり、このパソコン609はローカルエリアネットワーク602、603との間でデータの授受を行う。また、このパソコン609はカラープリンタ605等とローカルエリアネットワーク603または専用線を介して接続されている。610はファイルサーバで、ファイルサーバ607と同様の構成である。611はカラー複写機でファイルサーバ610と接続されている。

【0024】612はATMネットワーク601に接続されているデジタルテレビで、ATMネットワーク601を介して入力されるデータを受信し、これを復号して可視像としてディスプレイ装置に表示する。613はATMネットワーク601を介して入力されたデータを受

信するVTR、614はATMネットワーク601にデータを送出するCATV局、615はATMネットワーク601に他のATMネットワークを接続するためのルータ、616はローカルエリアネットワーク603を他のローカルエリアネットワークと接続するためのルータである。

【0025】また、ファクシミリ装置604とプリンタ605とカラー複写機607とATMネットワーク601との間には不図示のATMネットワークスイッチが設けられている。

【0026】また、これらの各機器には第1、第2の実施例に示した課金装置103、課金データベース101、累積金額記憶装置102等の課金手段が配置されているものとする。

【0027】次に動作について図8を用いて説明する。ここではCATV局614を送信側とし、デジタルテレビ612を受信側とした場合について説明する。まず、図8の1101で示すように、デジタルテレビ612は課金手段を介して、CATV局に送信要求を行い、同時に画像品位を要求する。次に1102で示すようにCATV局614は画像データを転送し、デジタルテレビ612が受信する。この時第1、第2の実施例で説明したように課金動作が実行されている。デジタルテレビ612は1103で示すようにデータの受信を終了したいとき送信終了要求を送る。CATV局614の課金装置103はこの終了要求に応じて前述の課金動作を終了する。次にCATV局614は1104で示す送信終了要求に応じて送信を終了する。そしてCATV局614の課金装置103は1105で示すようにデジタルテレビ612に料金を通知する。尚、双方向のデータ転送がある場合は、送受信が逆転した形で上述と同様の課金が行われる。

【0028】上述と同様の動作がCATV局614とデジタルテレビ612のみならず、他の各機器同志でも行われ、そのデータのやり取りに対して第1、第2の実施例と同様に課金できることは明らかである。

【0029】図7は本発明が適用されるマルチメディアネットワークシステムの一例を示す図である。図7において、701は高速公衆回線を用いたB-ISDN網、702はケーブルテレビ(CATV)網、703、704はローカルエリアネットワーク(LAN)、705は通信衛星、761、762は通信衛星705を介して情報通信を行う地上局、771、772はこれらの通信網を利用して映像情報、音声情報、その他様々なマルチメディア情報を提供してその対価を受け取る情報提供者、791~799は情報提供者771、772から提供される情報を利用して対価を支払う利用者である。B-ISDN網701、CATV網702、LAN703、704、通信衛星705は互いに接続され、相互に情報のやり取り(双方向通信)が可能であり、また、各情報提

供者771、772、利用者791～799は、これらの通信網のいずれかに接続されている。

【0030】また、情報提供者771、772は第1の実施例に示した送信側の課金手段を有し、利用者791～799も送信側の課金手段と同様のものを有している。ただし、双方向通信が可能であるので、情報提供者と利用者とは送信側と受信側の2つの課金手段を各々持てば、情報提供者が利用者になったり、利用者が情報提供者になることができる。この課金手段は各装置に内蔵されていたり、各装置とネットワークの間に挿入する形で設置されていたり、各装置の外付け装置として各装置に接続されていたりする。

【0031】次に、例えば利用者793を受信側とし、送信側を情報提供者772とした場合の動作について図8を用いて説明する。尚、図8に示す伝送路は、LAN2704、B-ISDN網701、CATV網702、LAN703、704に相当する。

【0032】図8において、1101で示すように受信側（利用者793）は課金手段を介して、送信側（情報提供者772）に送信要求を行い、同時に画像品位を要求する。次に1102で示すように、送信側はデータを転送し、受信側が受信する。この時第1、第2の実施例で説明したように課金動作が実行されている。受信側は1103で示すように、データの受信を終了したいとき送信終了要求を送る。送信側の課金装置はこの終了要求に応じて課金動作を終了する。次に送信側は送信終了要求1104に応じて送信を終了する。そして送信側の課金装置は1105で示すように受信側に料金を通知する。双方向のデータ転送がある場合は、送受信が逆転した形で上記と同様の課金が行われる。他の利用者と情報提供者との間の送受信についても同様の動作及び課金が行われる。以上のように広域ネットワークの中においても第1、第2の実施例と同様の課金を行うことができる。

【0033】次に本発明で用いられる暗号化について説明する。暗号化は”暗号とセキュリティ”、(辻井重男、笠原正雄、昭晃堂(1990))に記載されているように種々の方式があるが、現在よく使われている方式の例としてDESがある。DES暗号は米国商務省標準局でビジネス一般用に標準化された暗号方式で、そのアルゴリズムは公開されている。また、DES暗号を使用する時の利用モードも標準化されている。まずDESのアルゴリズムについて説明し、続いて利用モードについて説明する。

【0034】(A) DESのアルゴリズム

DES暗号では、64ビットのデータブロックを単位に暗号化及び復号が行われ、鍵の長さは56ビット(8ビットのパリティビットを加える64ビット)とされている。暗号アルゴリズムは転置式と換字式とを基本としており、これらの転置と換字を適当に組み合わせた処理を

16段繰り返すことにより、平文のビットパターンをかき混ぜ、意味の分からない暗号文に変換している。復号する場合は、逆にかき混ぜることにより、元の平文を復元する。

【0035】このかき混ぜかたのパラメータを56ビットの鍵で指定する。鍵の候補の数は2の56乗(約10の17乗)個であり、総当たりの解読、つまり入手した暗号文と平文のペアに対し、鍵を1回ずつ変化させてチェックする解読を行うと、1回のチェックに500nsかかるすると(128Mbpsの処理速度)、全体で1000年程度かかる計算になる。

【0036】DESのアルゴリズムの詳細は連邦情報処理規格に公表されている。図9にDESアルゴリズムの全体のブロック図を示す。前述のように、DESは64ビットの平文(あるいは暗号文)を入力し、56ビットの鍵のコントロールのもとに64ビットの暗号文(あるいは平文)を出力する暗号である。以下、DESの詳細を、(1)暗号処理、(2)復号処理、(3)暗号関数、(4)鍵のスケジューリングに分けて図9と共に説明する。

【0037】(1) 暗号化処理

暗号化処理では、まず64ビットの平文に対して転置(初期転置IP)が行われる。この初期転置は固定である。この転置処理の出力は途中複雑な16段の暗号化処理を経た後に最後に転置(最終転置IP⁻¹)が行われる。この最終転置も固定である。

【0038】初期転置が行われた64ビットのデータは、32ビットずつ左右に分割され左半分がL₀、右半分がR₀となる。このL₀とR₀からL₁₆とR₁₆になるまで16段にわたって図9に示す処理が行われる。つまり、n段目の処理を終了したときの左右の32ビットをそれぞれL_n、R_nとすると、L_n、R_nは次式で表されるものとなる。

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} \# f(R_{n-1}, K_n)$$

【0039】ここで、#はビット毎のmod 2の排他的論理和を意味し、K_nはn段目に入力される48ビットの鍵、L_{n-1}とR_{n-1}はそれぞれn-1段目の出力、fはR_{n-1}とK_nを用いて32ビットのデータを出力する関数である。このfについての詳細は後の(3)で述べる。

【0040】(2) 復号処理

暗号文から平文への復号処理も、平文から暗号文への暗号化処理と全く同じアルゴリズムを用いて行うことができる。復号は暗号化の逆変換を行えばよいわけだが、既に述べたように最終転置IP⁻¹は初期転置IPの逆変換となっており、さらに16段の各段において、

$$R_{n-1} = L_n$$

$$L_{n-1} = R_n \# f(L_n, K_n)$$

となるため、R_{n-1}とL_{n-1}を求めるためには、R_n、

L_n 、 K_n があれば同一の関数 f を用いることができる。従って、各段の変換において暗号化に用いられたのと同じ K_n を用いて処理を行えば復号が行えることになる。

【0041】具体的には、DESアルゴリズムに入力された暗号文は、初期転置 IP により L_{16} と R_{16} に変換される。これに1段目の処理では K_{16} を用いて L_{15} と R_{15} を得、次に K_{15} を用いて L_{14} と R_{14} を得るというように16段の処理を行い、 L_0 と R_0 を得る。最後に L_0 と R_0 を合成したものに最終転置 IP^{-1} を行えば、もとの平文が出力される。

【0042】(3) 暗号関数 $f(R, K)$

暗号関数 $f(R, K)$ を計算する方式を図10に示す。DESの暗号方式では、この $f(R, K)$ 以外の部分はすべて2進数演算で線形であるが、この $f(R, K)$ の変換が非線形であるため、暗号強度を高めている。32ビットの R は図11に示すように、まず拡大転置 E によって並び換えられると共に一部のビットは重複されて48ビットに拡大される。

【0043】この48ビットは同じ48ビットの鍵 K は排他的論理和の演算を施され、6ビットずつ8組に分割されて S_1 から S_8 までの8つのボックスに入力される。 S_1 から S_8 は選択関数または S ボックスと呼ばれており、6ビットを入力し、4ビットを出力する換字式の表である。1つの S ボックスには4種類の換字表が用意されており、それぞれ表中の行番号0、1、2、3に対応している。この4種類の換字表のどれを用いるかは、入力される6ビットのうち最初と最後のビットで決まり、選ばれた換字表に従って入力された6ビットの中央の4ビットが換字されることになる。8つの S ボックスからの出力32ビットは次に転置 P を行い、最終的な $f(R, K)$ の出力となる。

【0044】(4) 鍵のスケジューリング

(1) ~ (3) で示したように鍵は各段毎に48ビット必要であり、16段全部では $48 \times 16 = 768$ ビットの鍵が実質的に必要となる。DESアルゴリズムに入力される56ビットの鍵をもとにこれら K_1 から K_{16} まで16個の48ビットの鍵を生成する手順(スケジューリング)は以下になっている。

【0045】パリティビットを含む64ビットの入力鍵は転置(鍵の縮約型転置 $PC-1$) により、転置が行われると共にパリティビットが除かれた56ビットになる。この56ビットもまた2つに分割され上半分の28ビットが C_0 、下半分が D_0 となる。この C_0 と D_0 をそれぞれ左に順にシフトすることにより、 C_1 、 D_1 から C_{16} 、 D_{16} が順次生成される。 n 段目の鍵は、 C_n と D_n からなる56ビットを入力し、転置(鍵の縮約型転置 $PC-2$) を行って48ビットとなる。

【0046】(B) DESの利用モード

ブロック暗号の利用モードとしては、以下の4種類のモ

ードが提案されている。

1. ECB (Electric Codebook) モード
 2. CBC (Cipher Block Chaining) モード
 3. OFB (Output FeedBack) モード
 4. CFB (Cipher FeedBack) モード
- 【0047】以下にそれぞれのモードについて説明する。

(1) ECBモード

DESをブロック暗号としてそのまま用いる方法。

(2) CBCモード

64ビットのブロック単位で暗号化し、更にこの暗号文出力と次のブロックの平文との排他的論理和を次の暗号化の入力とする。これを繰り返して次々と連鎖させる。ECBモードに比べて暗号解読や能動的な不正行為に対して強化されている。DES暗号の利用モードの一つとして標準化されている。

【0048】(3) OFBモード

DES暗号の出力を入力にフィードバックすると同時に、出力のうちの何ビットかを疑似乱数として取り出すことを行い、DES暗号を乱数鍵生成器として利用したもの。取り出された疑似乱数はストリーム暗号の鍵として用いられる。DES暗号の鍵は固定である。DES暗号の利用モードの一つとして標準化されている。

【0049】(4) CFBモード

DES暗号の出力のうちの何ビットかを疑似乱数として取り出すことを行い、取り出された疑似乱数はストリーム暗号の鍵として用いられる。ただし、ストリーム暗号で暗号化された暗号文はDES暗号の入力としてフィードバックされる。これによりOFBモードに比べて、同期誤りが起こってもあるビット分だけが影響を受け、その後からは自動的に同期が回復できるという特徴を持つ。また、DES暗号の鍵は固定である。DES暗号の利用モードの一つとして標準化されている。

【0050】

【発明の効果】以上説明したように、本発明によれば、利用者に提供される画像の品位に応じて適正な課金を行うことができる。

【0051】また、利用者が望む画像品位を選択できるようにすることにより、さらに公平で適正な課金方式を実現できる。また、情報を暗号化することにより、課金情報のセキュリティが保たれ、改ざんやなりすまし等の不正行為から課金情報を守ることができる。

【0052】さらに、暗号処理時間を測定することにより、情報の受信時間に応じて適正な課金を行うことができる。

【図面の簡単な説明】

【図1】本発明の第1の実施例を示すブロック図である。

【図2】図1の課金データベースを示す構成図である。

【図3】図1の累積金額記憶装置を示す構成図である。

【図4】図1の課金装置を示す構成図である。

【図5】本発明の第2の実施例を示すブロック図である。

【図6】本発明を適用したネットワークシステムの構成図である。

【図7】本発明を適用したマルチメディアネットワークシステムの構成図である。

【図8】図6、図7におけるシステムの動作を示すシーケンスチャートである。

【図9】暗号化のアルゴリズムの一部を詳しく示したフローチャートである。

【図10】関数fの内容を示したフローチャートである。

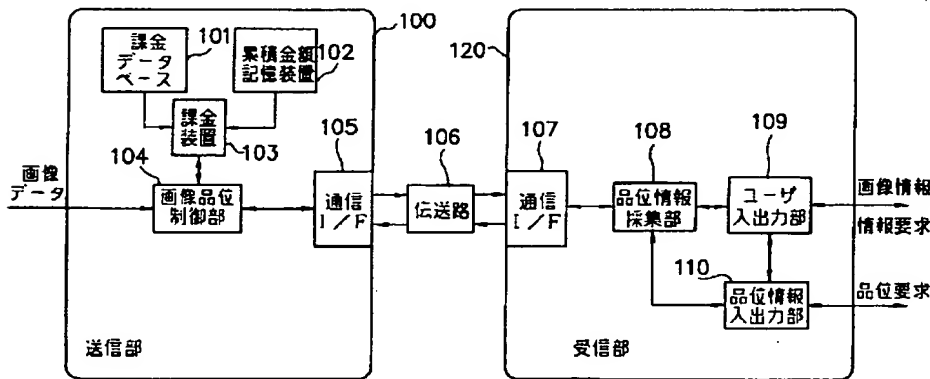
【図11】課金の手順の例を示したフローチャートである。

る。

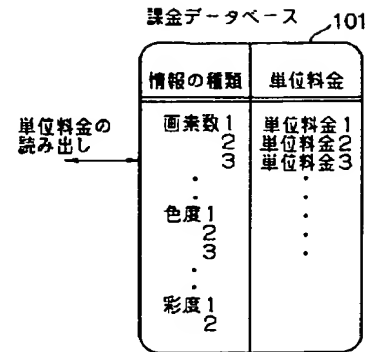
【符号の説明】

- 100 送信部
- 101 課金データベース
- 102 累積金額記憶装置
- 103 課金装置
- 104 画像品位制御部
- 105 通信インタフェース
- 107 通信インタフェース
- 108 品位情報採集部
- 109 ユーザ入出力部
- 110 品位情報入出力部
- 111 共通鍵暗号処理部
- 112 共通鍵暗号処理部
- 113 時間測定部
- 120 受信部

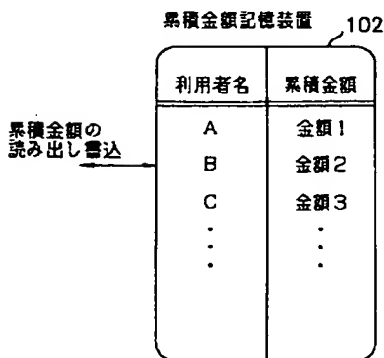
【図1】



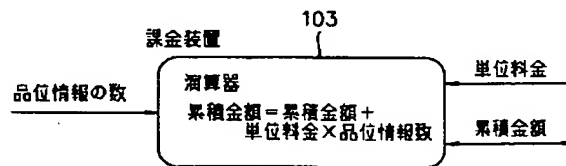
【図2】



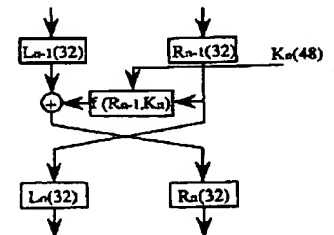
【図3】



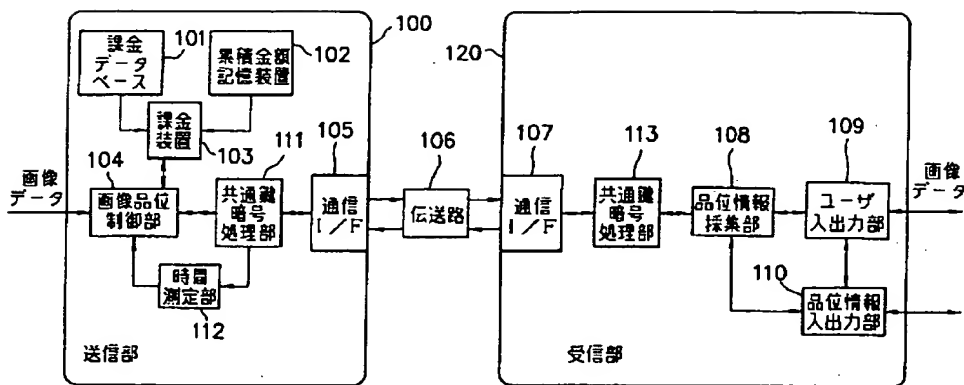
【図4】



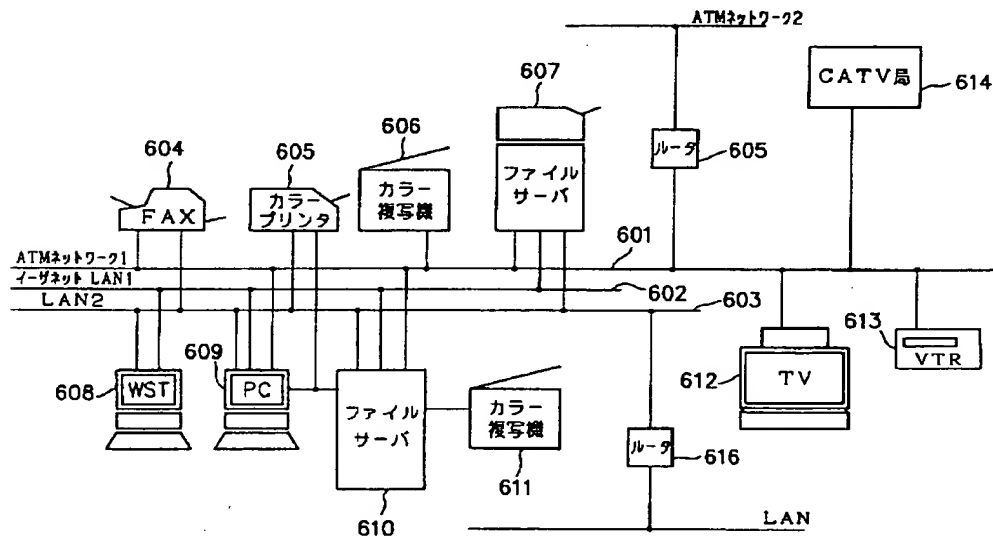
【図10】



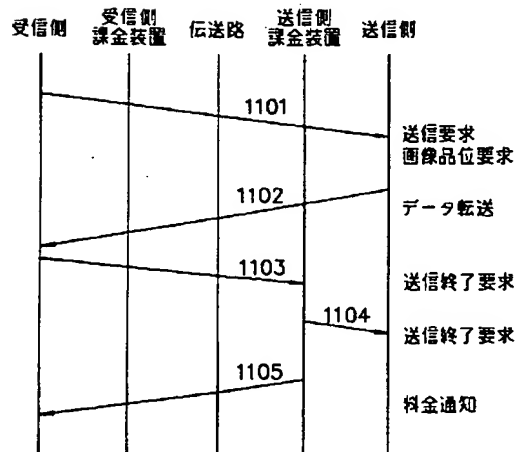
【図5】



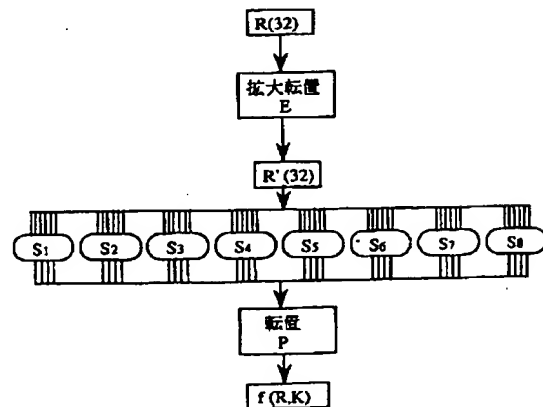
【図6】



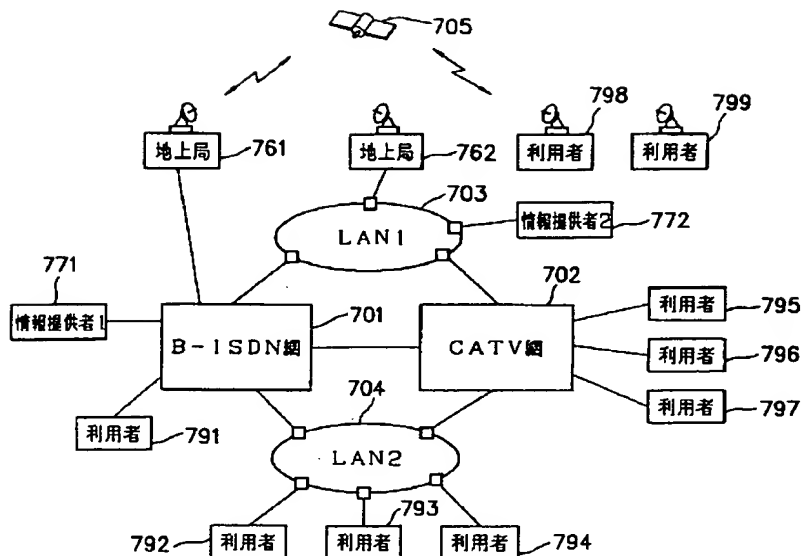
【図8】



【図11】



【図7】



【図9】

